## **WHAT IS CLAIMED IS:**

1	1.	A system for secure data transfer over a network, the system comprising:
2		memory;
3		a memory controller configured to transfer data received from the network
4	to the memor	ry; and
5		a processor, including:
6		logic configured to retrieve a portion of the data from the memory
7	using the me	mory controller;
8		logic configured to perform security operations on the retrieved
9	portion of the	e data; and
10		logic configured to store the operated-on portion of the data in the
11	memory usin	g the memory controller;
12		wherein the memory controller is further configured to transfer the
13	operated-on p	portion of the data from the memory to the network.
1	2.	The system of claim 1, comprising a network interface coupled to memory
2	controller, th	e network interface comprising:
3		a first data moving unit (DMU) configured to exchange secure data with a
4	first portion of	of the network; and
5		a second DMU configured to exchange non-secure data with a second
6	portion of the	e network.
1	3.	The system of claim 2, wherein the network interface comprises:
2		a first serializer/deserializer (SERDES) circuit coupled between the first
3	DMU and the	e first network portion and a second SERDES coupled between the second
4	DMU and the	e second network portion, each SERDES configured to convert serial data
5	received from	n the respective network portions to a parallel format and to convert parallel
6	data received	from the respective DMUs to a serial format.

1	4.	The system of claim 1, wherein the logic configured to perform security
2	operations comprises:	
3		logic configured to obscure the portion of the data when the retrieved
4	portion is no	n-secure data;
5		logic configured to decipher the portion of the data when the retrieved
6	portion is sec	cure data; and
7		logic configured to determine an integrity of the portion of data.
1	5.	The system of claim 1, wherein the processor comprises:
2		logic configured to perform quality-of-service (QoS) operations on the
3	data in coord	lination with performing the security operations.
1	6.	The system of claim 5, wherein the logic configured to perform QoS
2	operations co	omprises:
3		logic configured to identify an information flow associated with the
4	portion of the	e data;
5		logic configured to determine a priority of the information flow; and
6		logic configured to schedule at least one of the retrieving the portion of the
7	data and the	transferring the operated-on portion of the data from memory based on the
8	priority of th	e information flow associated with the portion of the data.
1	7.	The system of claim 6, wherein the processor comprises:
2		logic configured to decipher the portion of the data prior to the identifying
3	of the inform	nation flow when the retrieved portion is secure data; and
4		logic configured to obscure the portion of the data after the identifying of
5	the informati	on flow when the retrieved portion is non-secure data

1	8.	The system of claim 1, wherein the processor comprises:
2		logic configured to compress the portion of the data using the processor
3	prior to perfo	orming the security operations when the retrieved portion is non-secure data;
4	and	
5		logic configured to decompress the portion of the data in the processor
6	after perform	ning the security operations when the retrieved portion is secure data.
1	9.	The system of claim 1, wherein the memory includes a memory block
2	having a plu	rality of memory banks, the memory controller comprising:
3		logic configured to reference the plurality of memory banks in a sequence
4	that minimiz	tes a memory access time.
1	10.	The system of claim 1, wherein the memory controller comprises:
2		logic configured to include a request to reference the memory into one of a
3	group of read	d requests and a group of write requests; and
4		logic configured to execute all requests included in one of the groups of
5	read requests	s and write requests before executing a request included in the other group.
1	11.	The system of claim 10, comprising:
2		logic configured to include error correction code with the data transferred
3	to or stored in the memory; and	
4		logic configured to detect and correct errors in the data retrieved or
5	transferred f	from the memory based on the error correction code included with the data.
1	12.	A method for secure data transfer over a network, the method comprising:
2		transferring data from the network to memory using a memory controller;
3		retrieving a portion of the data from the memory into a processor using the
4	memory con	troller;

5		performing security operations on the retrieved portion of the data using
6	the processor	· • • • • • • • • • • • • • • • • • • •
7		storing the operated-on portion of the data in the memory using the
8	memory cont	roller; and
9		transferring the operated-on portion of the data from the memory to the
10	network usin	g the memory controller.
1	13.	The method of claim 12, wherein the security operations comprise at least
2	one of:	
3		obscuring the portion of the data when the retrieved portion is non-secure
4	data;	
5		deciphering the portion of the data when the retrieved portion is secure
6	data; and	
7		determining an integrity of the portion of data.
1	14.	The method of claim 12, comprising:
2		performing quality-of-service (QoS) operations on the data in coordination
3	with perform	ing the security operations using the processor.
1	15.	The method of claim 14, wherein the QoS operations comprise:
2		identifying an information flow associated with the portion of the data;
3		determining a priority of the information flow; and
4		scheduling at least one of the retrieving the portion of the data and the
5	transferring t	he operated-on portion of the data from memory based on the priority of the
6	information f	low associated with the portion of the data.

i	16.	The method of claim 15, comprising:
2		deciphering the portion of the data prior to the identifying of the
3	information fl	ow when the retrieved portion is secure data; and
4		obscuring the portion of the data after the identifying of the information
5	flow when the	e retrieved portion is non-secure data.
1	17.	The method of claim 12, comprising:
2		compressing the portion of the data using the processor prior to
3	performing th	e security operations when the retrieved portion is non-secure data; and
4		decompressing the portion of the data in the processor after performing the
5	security opera	ations when the retrieved portion is secure data.
1	18.	The method of claim 12, comprising:
2		including a request to reference the memory into one of a group of read
3	requests and a	group of write requests; and
4		executing all requests included in one of the groups of read requests and
5	write requests	before executing a request included in the other group.
1	19.	The method of claim 18, wherein the executing all requests included in
2	one of the gro	ups of read requests and write requests occurs when a sum of the requests
3	included in or	ne of the groups corresponds to a predetermined amount of the memory.
1	20.	The method of claim 12, comprising:
2		including error correction code with the data transferred to or stored in the
3	memory; and	
4		at least one of detecting and correcting errors in the data retrieved or
5	transferred fro	om the memory based on the error correction code included with the data

1	21.	The method of claim 12, comprising.
2		referencing portions of the memory in a sequence that minimizes a
3	memory acce	ess time.
1	22.	A computer readable medium containing a computer program for secure
2		•
3	data transfer over a network, wherein the computer program comprises executable instructions for:	
	mstructions i	
4		transferring data from the network to memory using a memory controller;
5		retrieving a portion of the data from the memory into a processor using the
6	memory controller;	
7		performing security operations on the retrieved portion of the data using
8	the processor;	
9		storing the operated-on portion of the data in the memory using the
10	memory controller; and	
11		transferring the operated-on portion of the data from the memory to the
12	network usin	g the memory controller.
1	23.	The computer readable medium of claim 22, wherein the computer
2	program com	nprises executable instructions for:
3	1 0	obscuring the portion of the data when the retrieved portion is non-secure
4	data;	3
5	<b></b> ,	deciphering the portion of the data when the retrieved portion is secure
6	data; and	designering the portion of the data when the retareved portion is seeme
7	data, and	determining an integrity of the portion of data.
/		determining an integrity of the portion of data.
1	24.	The computer readable medium of claim 22, wherein the computer
2	program com	nprises executable instructions for:

3		performing quality-of-service (QoS) operations on the data in coordination
4	with perform	ing the security operations using the processor.
1	25.	The computer readable medium of claim 24, wherein the computer
2	program con	prises executable instructions for:
3		identifying an information flow associated with the portion of the data;
4		determining a priority of the information flow; and
5		scheduling at least one of the retrieving the portion of the data and the
6	transferring t	the operated-on portion of the data from memory based on the priority of the
7	information	flow associated with the portion of the data.
1	26.	The computer readable medium of claim 22, wherein the computer
2	program comprises executable instructions for:	
3		compressing the portion of the data using the processor prior to
4	performing t	he security operations when the retrieved portion is non-secure data; and
5		decompressing the portion of the data in the processor after performing the
6	security oper	rations when the retrieved portion is secure data.